STUDENT HANDOUT · WEEK 4

Threat Actors, Threat Vectors, and Attack Surfaces

SY0-701 objectives 2.1, 2.2. Notes, exercises, review questions, and the lab.

Name	
Date	

THIS WEEK YOU WILL

1. Compare the six threat actor types by location, resources, and sophistication.
2. Match an incident to the most likely threat actor and motivation.
3. Identify message, image, file, voice, and removable device threat vectors.
4. Explain how vulnerable software, unsupported systems, open ports, and defaults widen the attack surface.
5. Recognize phishing, vishing, smishing, BEC, pretexting, impersonation, and related techniques.
6. Read an email's headers and links to decide whether it is a phish.

KEY IDEAS

Six kinds of threat actors

Nation-state	Government-backed; the best funded and most patient. (Advanced persistent threat)
Unskilled attacker	Runs tools and scripts that others wrote. (A downloaded DDoS tool)
Hacktivist	Attacks to promote a political or social cause. (A defaced city website)
Insider threat	A trusted person who misuses their access. (A clerk selling records)
Organized crime	Profit-driven groups run like businesses. (A ransomware gang)
Shadow IT	Technology adopted without IT's approval. (A personal cloud drive)

Location, money, and skill set actors apart

Actor	Internal or external	Resources	Sophistication
Nation-state	External	Very high: government budgets	Very high: custom tools, zero-days
Organized crime	External	High: crime profits fund it	High
Hacktivist	External, sometimes internal	Low to moderate	Low to high
Insider threat	Internal	Uses access already granted	Varies; access matters more
Unskilled attacker	External	Low	Low: relies on others' tools
Shadow IT	Internal	Low: often a personal account	Low; usually not malicious

What drives an attack

Gain and advantage	Belief and grievance
Financial gain: ransom, fraud, theft	Philosophical or political beliefs
Data exfiltration: steal data to sell or use	Ethical: expose wrongdoing or find flaws
Espionage: secrets for a state or a rival	Revenge: a grudge against the organization
Blackmail: pay, or we publish what we took	Disruption or chaos: harm for its own sake
War: damage an enemy's systems	Service disruption: knock a service offline

Most attacks arrive as a message or a file

Vector	How the attack arrives	Example
Message-based	Email, SMS text, or instant message	A fake invoice email with a link
Image-based	A link or code hidden in an image	A QR code that opens a fake login
File-based	A document, PDF, or archive carries it	A macro in an Office document
Voice call	A caller talks the victim into acting	A fake IT help desk call
Removable device	USB drives and other media carry malware	A USB stick left in the parking lot

Weak systems widen the attack surface

Surface	Why it is a risk
Vulnerable software	Unpatched flaws, client-based or agentless
Unsupported systems	The vendor no longer releases patches
Unsecure networks	Open Wi-Fi, live wall jacks, Bluetooth
Open service ports	Every listening service is a possible way in
Default credentials	Factory passwords anyone can look up
Supply chain	MSPs, vendors, and suppliers with access

Social engineering targets people

Phishing	Fraudulent email that lures a click, reply, or login. (Fake password reset)
Vishing	Phishing by voice call, often with a spoofed number. (Fake bank fraud team)
Smishing	Phishing by SMS text message. (Package held: pay a fee)
Impersonation	Pretending to be someone the victim trusts. (Posing as the IT vendor)
Email compromise (BEC)	Uses a trusted business email account to steal money. (New bank details for AP)
Pretexting	A made-up story that gives a request a reason. (Audit needs the list today)

Attacks that borrow trusted sites and names

Technique	How it works	Example
Watering hole	Infect a site the target group already visits	A medical association site serving malware
Brand impersonation	Copy a known brand's look to win trust	A fake bank login page with the real logo
Typosquatting	Register a lookalike of a real domain	lakesideclinlc.example for lakesideclinic
Misinformation	False information shared without intent	A wrong virus rumor forwarded by staff
Disinformation	False information spread on purpose	A fake breach notice linking to a scam

Reading a suspicious email like an analyst

1. Sender	Compare From, Reply-To, and Return-Path
2. Route	Read the Received headers from the bottom up

3. Authentication	Check the SPF, DKIM, and DMARC results
4. Links	Compare the shown text with the real address
5. Attachments	Note the file type and any double extension
6. Report	Report it, then block the sender and domain

EXERCISE 1: NAME THE ACTOR AND THE MOTIVE

8 MINUTES · PAIRS

For each incident, name the most likely threat actor, its main motivation, and whether it is internal or external.

#	Prompt	Your answer
1	Ransomware locks a clinic's files and demands $80,000	
2	A fired billing clerk deletes invoices with a login never disabled	
3	A teenager floods a school website with a tool from a forum	
4	Malware quietly copies a defense contractor's designs for months	
5	A city website is defaced over a vote on a new pipeline	
6	Nurses share patient photos through a personal messaging app	
7	Power grid systems are wiped during an armed conflict	
8	Thieves steal records and threaten to publish them unless paid	

EXERCISE 2: NAME THE VECTOR OR THE TECHNIQUE

10 MINUTES · SMALL GROUPS

For each event, name the threat vector or social engineering technique, and one control that would have stopped it.

#	Prompt	Your answer
1	A text says a package is held and links to a fee payment page	
2	A caller claiming to be the EHR vendor asks for an admin password	
3	The CFO's hacked mailbox tells payables to change a vendor's bank	
4	A man says he is the copier technician and needs the closet key	
5	A nurse mistypes the portal address and lands on a lookalike site	
6	A regional nurses' forum is altered to serve malware to visitors	
7	A USB drive labeled Payroll 2026 is found in the clinic lobby	
8	The new Wi-Fi printer still uses the admin password admin	
9	The clinic's IT provider is breached; its remote tool spreads malware	

REVIEW QUESTIONS

1. What separates an insider threat from shadow IT?

2. What is the difference between misinformation and disinformation?

3. Why is an unsupported operating system riskier than a supported one that is a month behind on patches?

4. An email header shows dmarc=fail. What does that suggest?

5. A caller posing as a doctor locked out before surgery pressures the help desk to reset a password. Name two techniques.

KEY TAKEAWAYS

- **Know the actor.** Funding, skill, and access shape what each kind of attacker can do.
- **Motive predicts the target.** Money, secrets, belief, and grudges each point to different assets.
- **Shrink the attack surface.** Patch, retire unsupported systems, close ports, and change defaults.
- **People are a vector too.** Check the sender, the route, and the links before acting on a request.

LAB 4: PHISHING EMAIL HEADER AND LINK ANALYSIS

60 MINUTES

Use the Linux VM from Lab 1 on its host-only network, and the sample email file for this lab, [sample-phish.eml](/courses/security-plus/files/sample-phish.eml) (download it on your host computer and copy it into the VM through a VirtualBox shared folder, or briefly switch the VM's adapter to NAT to download it and switch it back afterward), which is a harmless sample built for the course. Never open the sample in a mail client, never visit any link in it, and do not look up or visit live phishing sites; all analysis is done by reading text.

Steps

1. Make a new folder with mkdir ~/lab4, copy sample-phish.eml into it, and move into it with cd ~/lab4. View the file as plain text with less sample-phish.eml. Note the subject, the claimed sender, and what the message asks the reader to do.
2. Separate the headers from the body with sed '/^$/q' sample-phish.eml > headers.txt. The headers end at the first blank line.
3. Compare the sender fields with grep -iE '^(From|Reply-To|Return-Path|Date|Message-ID):' headers.txt. Record every domain you see and whether they match.
4. Trace the route with grep -i -A2 '^Received:' headers.txt. Read the Received lines from the bottom up and record the first server and IP address that handled the message.
5. Read the authentication results with grep -i -A3 'Authentication-Results' headers.txt. Record the SPF, DKIM, and DMARC results and what each one means.
6. Pull every link from the body with grep -oiE 'href="[^"]+"' sample-phish.eml | sort -u. For each, compare the real address with the text the reader sees, and look for lookalike domains, misspellings, or shorteners. Write each link down defanged, for example hxxps://example[.]com.
7. List any attachments with grep -iE 'filename=|Content-Type:' sample-phish.eml. Note each file name, its type, and any double extension.
8. Write a verdict: phishing or legitimate. List at least five indicators that support it, each tied to a line of the header or body, and name the social engineering techniques used.
9. Write three recommendations for Lakeside Family Clinic that would block or blunt this message, such as a DMARC policy, a filtering rule, or a reporting step for staff.

Hand in

A one-to-two page analysis report: a table of the header fields you examined and what each showed, the defanged links with your assessment of each, your verdict with at least five supporting indicators, and three recommendations for the clinic.

Questions to answer in your report

1. Which single header finding was the strongest evidence of spoofing, and why is it harder to fake than the From line?

2. Explain in your own words what SPF, DKIM, and DMARC each check, and what the clinic would gain by publishing a DMARC policy of reject.
3. Which social engineering techniques and pressure tactics did the sample use? Quote the words in the body that show them.
4. Why should analysts defang links in reports and avoid visiting suspected phishing sites, even from a lab VM?